Bezpečnostný projekt

ochrany osobných údajov

Názov organizácie: Slovenský rýchlokorčuliarsky zväz

Sídlo: Za Hornádom 15/1, 052 01 Spišská Nová Ves

Dátum spracovania: 1.5.2017

**Účel a cieľ**

Cieľom bezpečnostného projektu je vymedziť rozsah a spôsob technických, organizačných a personálnych opatrení potrebných a realizovaných na eliminovanie a minimalizovanie hrozieb pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti, funkčnosti a ochrany osobných údajov.

Bezpečnostné vlastnosti, ktoré informačný systém osobných údajov musí mať:

* dôvernosť – vlastnosť, že informácia nie je dostupná alebo prístupná neautorizovaným jednotlivcom, technickým prostriedkom, alebo procesom,
* integrita dát – ochrana dát pred zmenou alebo zničením neautorizovaným spôsobom,
* integrita systému – vlastnosť, že systém vykonáva svoju zamýšľanú funkciu nenarušeným spôsobom, bez zámernej alebo náhodnej neautorizovanej manipulácie so systémom,
* dostupnosť – vlastnosť, že niečo je na požiadanie prístupné a použiteľné autorizovanou entitou,
* individuálna zodpovednosť – vlastnosť zaručujúca, že činnosti určitej entity môžu byť sledované jedinečne pre túto entitu,
* autenticita – vlastnosť zaručujúca, že identita subjektu alebo zdroja je taká, za akú je prehlasovaná; autenticita sa aplikuje na užívateľov, procesy, systémy a informácie,
* spoľahlivosť – vlastnosť zaručujúca konzistentný režim práce, zamýšľané správanie a jeho výsledky.

Bezpečnostný projekt je spracovaný v súlade so zákonom č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a vyhlášky č. 164/2013 Z. z. Úradu na ochranu osobných údajov. Pri analýze a návrhu bezpečnostných opatrení boli použité metodika a postupy popísané v technickej norme STN ISO/IEC 27001 Informačné technológie, Bezpečnostné metódy, Systémy riadenia informačnej bezpečnosti, Požiadavky a STN ISO/IEC 27005 Informačné technológie, Bezpečnostné metódy, Riadenie rizík informačnej bezpečnosti.

**Definícia pojmov**

Osobné údaje – údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takouto osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

Spracúvanie osobných údajov – vykonávanie akýchkoľvek operácií alebo súboru operácií s osobnými údajmi, napr. ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.

Prevádzkovateľ – každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene; ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto spĺňa ustanovené podmienky. Prevádzkovateľom je Slovenský rýchlokorčuliarsky zväz.

Sprostredkovateľ – každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve.

Oprávnená osoba – každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu s občianskym združením Slovenský rýchlokorčuliarsky zväz a ktorá spracúva osobné údaje v rozsahu a spôsobom určenom v poučení v zmysle zákona o ochrane osobných údajov.

Dotknuté osoby – každá fyzická osoba, o ktorej sa spracúvajú osobné údaje.

Informačný systém osobných údajov – je informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe (ďalej len „informačný systém“); informačným systémom sa na účely tohto zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.

Automatizované prostriedky spracúvania – (ďalej len „APS“) súhrn technických prostriedkov výpočtovej techniky, operačné systémy a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením určeným na automatizované spracovanie údajov.

Aktíva – jednotlivé časti informačných systémov osobných údajov, automatizovaných prostriedkov spracúvania a osobné údaje v elektronickej a písomnej forme.

Zraniteľnosť – zahrňuje slabé miesta aktíva alebo skupiny aktív, ktoré môžu byť využité hrozbou.

Hrozba – potenciálna príčina nežiaduceho incidentu.

Riziko – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktív alebo skupiny aktív a spôsobí tak stratu alebo zničenie aktív.

Zvyškové riziko – riziko, ktoré zostáva po implementácii bezpečnostných opatrení.

Bezpečnostné opatrenie – vykonávaná prax, pracovný postup alebo zariadenie, ktoré znižujú riziko.

Bezpečnostný incident – neočakávaná alebo nežiaduca udalosť, ktorá môže ohroziť bezpečnosť osobných údajov.

Dopad – výsledok nežiaduceho bezpečnostného incidentu.

**Bezpečnostný zámer**

Bezpečnostný zámer špecifikuje požiadavky na bezpečnosť informačných systémov a ciele, ktoré sa majú dosiahnuť na ochranu informačných systémov pred ich ohrozením.

Všeobecné bezpečnostné ciele sú:

* ochrana bezpečnosti a zdravia pri práci,
* ochrana majetku,
* ochrana finančných prostriedkov,
* ochrana osobných údajov,
* ochrana utajovaných informácií,
* ochrana dobrého mena organizácie,
* ochrana proti živelným pohromám.

Automatizované prostriedky spracúvania predstavujú koncentráciou cenných a dôležitých informácií významnú hodnotu. Súčasťou základných bezpečnostných cieľov je stanoviť základné postupy pre činnosť používateľov automatizovaných prostriedkov spracúvania.

***Základné bezpečnostné ciele***

Základné bezpečnostné ciele pri spracúvaní osobných údajov sú:

* vybudovať a trvalo udržiavať vysokú úroveň ochrany osobných údajov,
* chrániť osobné údaje všetkých dotknutých osôb pred zneužitím, odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním,
* chrániť práva fyzických osôb pred neoprávneným zasahovaním do ich súkromného života pri spracúvaní ich osobných údajov.

***Minimálne požadované bezpečnostné opatrenia***

Požadované bezpečnostné opatrenia sú:

* pri získavaní osobných údajov zamestnancov používať dotazník, ktorého súčasťou je dohoda, že zamestnanec je povinný oznámiť zmenu osobných údajov,
* pri automatizovanom spracúvaní osobných údajov používať programové vybavenie, ktoré vyžaduje meno a heslo užívateľa,
* údaje pravidelne zálohovať,
* používať antivírovú ochranu,
* zabezpečiť osobné údaje pred sprístupnením a zverejnením prostredníctvom zneužitia pripojenia do internetu,
* priestory, určené pre spracúvanie osobných údajov zamykať mimo pracovnej doby, chrániť priestory určené na spracúvanie osobných údajov,
* poučiť zamestnancov o povinnostiach súvisiacich s ochranou osobných údajov,
* písomné dokumenty archivovať tak, aby bol vedený zoznam dokumentov, miesto ich uloženia a zabezpečené vhodné podmienky na uloženia,
* nepotrebné písomné dokumenty likvidovať skartovaním, zabezpečiť dôslednú likvidáciu všetkých osobných údajov, ktoré už nie je potrebné spracúvať,
* uplatňovať bezpečnostné princípy práce s automatizovanými prostriedkami spracúvania.

**Analýza bezpečnosti informačných systémov**

***Bezpečnostné štandardy***

Ochrana aktív - všetkých dôležitých častí procesu spracúvania osobných údajov - závisí od vykonaných bezpečnostných opatrení vyplývajúcich z analýzy bezpečnosti informačného systému osobných údajov.

Podrobná analýza bezpečnosti spracúvaných údajov je časovo i finančne veľmi náročná, pri jej vykonávaní sa prihliada k druhu spracúvaných údajov, prípadne stupňu utajenia a podobne.

V zmysle zákona č. 122/2013 Z. z. je prevádzkovateľ povinný prijať primerané bezpečnostné opatrenia na ochranu osobných údajov pred ich zneužitím, odcudzením, neoprávneným prístupom, zmenou a rozširovaním. Z dôvodu primeranosti bola analýza rizík vykonaná neformálne, podľa technickej normy STN ISO/IEC 27005, takzvanou metódou pragmatického prístupu.

Metóda vychádza zo znalosti prostredia a zo skúsenosti jednotlivcov, nie je založená na presne definovaných metodológiách.

Uvedený štandard určuje postup podľa nasledovných štyroch krokov:

* špecifikácia rizík, určenie oblastí hrozieb pre spracúvané údaje a funkcionalitu systému,
* určenie miery rizika a definovanie jeho dopadu pre informačný systém,
* výber a návrh opatrení, ktoré definované riziká eliminujú, prípadne zmiernia ich dopad,
* posúdenie zvyškových rizík s dôrazom na pomer ceny bezpečnostných opatrení k hodnote spracúvaných údajov.

***Popis informačných systémov osobných údajov***

Množstvo a typy spracúvaných osobných údajov nepredstavujú svojou kvalitou dôležitý cieľ. Pravdepodobnosť úmyselného útoku na bezpečnosť osobných údajov je veľmi malá.

Podrobný zoznam spracúvaných osobných údajov a právny základ spracúvania sú uvedené v príslušných evidenciách jednotlivých informačných systémov.

**Personalistika a mzdy** - obsahuje osobitnú kategóriu osobných údajov

Účelom spracúvania osobných údajov je viesť personálnu a mzdovú agendu v súlade so zákonnými ustanoveniami. Počet dotknutých osôb tvorí aktuálny stav zamestnancov 4, archívne záznamy o bývalých zamestnancoch a rodinní príslušníci (vyživované osoby).

Spracúvajú sa tieto osobné údaje: meno, priezvisko, titul, rodné priezvisko, bydlisko, dátum a miesto narodenia, rodné číslo, pohlavie, číslo občianskeho preukazu, rodinný stav, národnosť, štátna príslušnosť, mená, dátum narodenia a rodné čísla detí a manželky, bydlisko detí a manžela/lky, dosiahnuté vzdelanie, predchádzajúci zamestnávatelia a odpracované roky, pracovné zaradenie, výška mzdy, číslo osobného účtu, zdravotný stav, zmenená zdravotná schopnosť, zdravotné prehliadky, zdravotná poisťovňa, doplnková dôchodková poisťovňa.

Osobné údaje v informačnom systéme Personalistika a mzdy manuálne a v elektronickej forme spracúva účtovník a predseda SRZ. Na spracovanie osobných údajov je vyčlenená samostatná kancelária, rozmiestnenie nábytku zabraňuje odpozeraniu osobných údajov. Osobné údaje získava osobným pohovorom a kopírovaním úradných dokladov a dokumentov o vzdelaní (občiansky preukaz, preukaz zdravotnej poisťovne, osvedčenia o odbornej spôsobilosti). Aktuálne osobné spisy má účtovník uložené u seba v kancelárii v uzatvorenej skrini.

Plnenie povinností prevádzkovateľa v oblasti BOZP a pracovnej zdravotnej služby na základe písomnej zmluvy zabezpečuje externý dodávateľ Mgr. Ambróz Koňak. Účtovník je oprávnený v nevyhnutnom rozsahu poskytovať tejto firme osobné údaje zamestnancov pre potreby vzdelávania a evidencie pracovných úrazov.

Osobné údaje sú poskytované na základe osobitných zákonov, ktoré sú uvedené v evidenčnom liste informačného systému.

**Členovia združenia -** obsahuje osobitnú kategóriu osobných údajov

Osobné údaje členov občianskeho združenia spracúvajú predseda SRZ. Údaje získava z prihlášok, spracúvajú sa tieto osobné údaje: meno, priezvisko, titul, dátum a miesto narodenia, rodné číslo, štátna príslušnosť, adresa trvalého pobytu alebo obdobného pobytu, adresa na doručovanie, adresa elektronickej pošty, číslo bankového účtu, druh športu.

Osobné údaje sú v informačnom systéme spracúvané na základe zákona č. 83/1990 Zb. o združovaní občanov a zákona č. 440/2015 Z. z. o športe a o zmene a doplnení niektorých zákonov.

**Účtovné doklady**

V informačnom systéme spracúva osobné údaje účtovník. Spracúva osobné údaje zamestnancov a členov združenia. Na spracúvanie používa aplikáciu Pohoda. Predseda SRZ zverejňuje na základe zákona č. 211/2010 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov predpísané údaje. Spracúvajú sa tieto osobné údaje: meno, priezvisko, titul, bydlisko.

Právnym základom spracúvania sú: zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, zákon č.222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, zákon č. 283/2002 Z. z. o cestovných náhradách v znení neskorších predpisov, zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach s príjmov v znení neskorších predpisov a zákon č. 440/2015 Z. z. o športe a o zmene a doplnení niektorých zákonov.

**Evidencia pošty**

Generálny sekretár spracúva osobné údaje odosielateľov a prijímateľov korešpondencie za účelom evidencie odoslanej a došlej pošty. Údaje o došlej pošte manuálne zapisuje do Registratúrneho denníka. Osobné údaje sa získavajú z obálok došlej pošty a obsahu korešpondencie. Spracúvajú sa tieto osobné údaje: meno, priezvisko, adresa, názov firmy.

Osobné údaje sa spracúvajú v informačnom systéme na základe zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

**Registratúra**

Písomné dokumenty určené na dlhodobé uloženie – registratúrne záznamy sú uložené v Registratúrnom stredisku. Správu registratúry vykonáva generálny sekretár, postup určuje Registratúrny poriadok.

Osobné údaje sa spracúvajú v informačnom systéme na základe zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

***Analýza a hodnotenie rizík***

Udalosti, ktoré môžu mať nepriaznivý účinok na bezpečnosť spracúvania osobných údajov alebo funkčnosť spracúvania môžu byť prírodné alebo ľudského pôvodu, môžu byť náhodné alebo úmyselné:

* prírodné vplyvy (záplavy, požiare, víchrice, blesky, zemetrasenia),
* nehody (strata, technická porucha, havária, ...),
* zanedbanie (nevykonať niečo, nesprávny postup, oneskorenie výkonu, ...),
* neetické konanie (korupcia, konflikt záujmov, špionáž, ...),
* kriminalita (krádež, násilie, podvod, sabotáž, terorizmus, ...).

Pravdepodobnosť výskytu týchto udalostí je rôzna a cieľom bezpečnostných opatrení je ich úplne odstrániť, alebo čo najviac obmedziť možnosti pre ich uskutočnenie.

Popis jednotlivých časti (aktív) informačného systému osobných údajov obsahuje hodnotenie možného rizika.

**Fyzická bezpečnosť**

Organizácia sídli v samostatnej prenajatej kancelárii v športovej hale, v oddelenej administratívnej časti, ktorá je chránená elektronickým zabezpečovacím systémom (EZS). Vstup do haly a do administratívnych priestorov je monitorovaný kamerovým systémom a je označený ako monitorovaný. Kamerový systém prevádzkuje vlastník budovy Správa telovýchovných zariadení Spišská Nová Ves (STEZ). Každý zamestnanec má Kľúč od vchodu a svoj vlastný kód. Narušenie priestorov EZS hlási na políciu. Správu kódov vykonáva dodávateľ systému spoločnosť DOBRO, spol. s r.o. Ďalšie priestory v športovej hale využíva STEZ, volejbalový klub, basketbalový klub a Spišský oblastný futbalový zväz. Spoločný vstup cez hlavný vchod do budovy haly je počas pracovnej doby odomknutý. Na dispečingu športovej haly, kde je celodenná služba, je v zapečatenej obálke uložený záložný kľúč od hlavného vchodu. Osobné údaje sa spracúvajú v samostatných kanceláriách. Osobné spisy zamestnancov sú uložené v uzamknutej skrini. Návštevy a externí dodávatelia sa môžu v administratívnych priestoroch pohybovať len pod dohľadom.

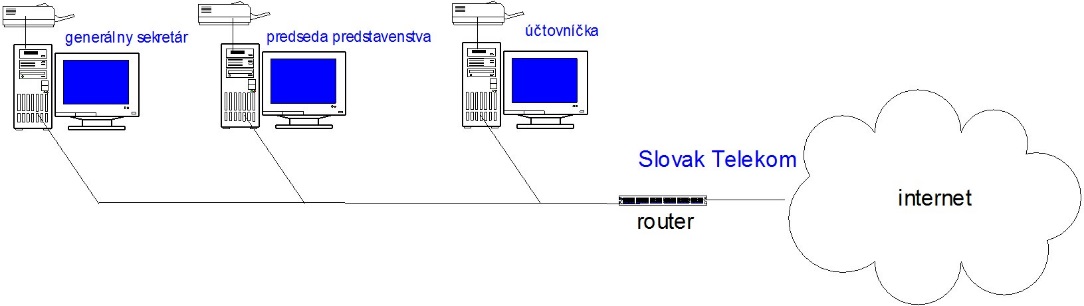
*Hodnotenia rizika:*

Organizačné zabezpečenie všetkých činností a preventívnych opatrení je na dostatočnej úrovni. Pravdepodobnosť krádeže prostriedkov automatizovaného spracúvania a písomných dokumentov je veľmi malá.

**Automatizované prostriedky spracúvania**

Na počítačoch, ktoré sa používajú na spracovanie osobných údajov, je nainštalovaný operačný systém MS Windows 7 Professional, spustenie osobných počítačov vyžaduje meno užívateľa a heslo, ku každému je pripojená lokálna tlačiareň.

Osobné údaje v informačnom systéme Personalistika a mzdy a Účtovné doklady sa spracúvajú v aplikácii Pohoda. Program MS WORD sa používa na vytváranie dokumentov, ktoré je potrebné vytlačiť (pracovné zmluvy). Spustenie aplikácie Pohoda vyžaduje meno užívateľa a heslo, prístup má len účtovníčka. Zálohovanie dát účtovník vykonáva pravidelne mesačne na USB disk. Na spracovanie evidencie členov združenia sa používa program MS WORD.

****

V počítačovej sieti sú zapojené celkom 3 osobné počítače. Router, ktorý slúži na pripojenie do siete MsÚ SNV, je umiestnený v kancelárii generálneho sekretára. Na osobných počítačoch je nainštalovaný antivírový program ESET, aktualizácia sa vykonáva automaticky z internetu.Na podporu dodávaného programového vybavenia Pohoda je s dodávateľom podpísaná zmluva, ktorá definuje podmienky starostlivosti a servisu. Zmluva je dodržiavaná, pravidelne sa vykonáva aktualizácia aplikácie. Združenie používa len legálne nadobudnutý softvér.

*Hodnotenie rizika:*

Používané technické vybavenie je na dostatočnej úrovni a súčasná starostlivosť o techniku zaručuje dostatočnú spoľahlivosť a malé riziko technickej poruchy, ktorá však v žiadnom prípade nebude mať za následok zničenie osobných údajov. Nie je žiaden predpoklad, že by chybou programového vybavenia mohlo dôjsť k ohrozeniu bezpečnosti osobných údajov. Sieťové služby sú nastavené na dostatočne vysokú mieru bezpečnosti, prienik z vonkajšej siete je veľmi málo pravdepodobný. Antivírový program je pravidelne aktualizovaný, riziko prieniku počítačových vírusov a ohrozenia bezpečnosti osobných údajov je veľmi malé. Používané technické a programové prostriedky pre zálohovanie vyhovujú množstvu spracúvaných osobných údajov. Realizované technické riešenia a princípy práce zabezpečujú dostatočne vysokú ochranu osobných údajov.

***Interné predpisy***

Smernica Ochrana osobných údajov určuje povinnosti všetkých oprávnených osôb pri používaní automatizovaných prostriedkov spracúvania. Registratúrny poriadok určuje postupy pre manipuláciu s písomnými dokumentami, lehotu ich uloženia a postup likvidácie.

***Špecifikácia použitých bezpečnostných opatrení***

V súvislosti s doterajšou prevádzkou organizácie už boli prijaté nasledujúce bezpečnostné opatrenia.

**Technické opatrenia** sa realizujú najmä použitím technických prostriedkov na zabránenie prístupu osôb do chránených priestorov. V oblasti informačných technológií sa tieto opatrenia vykonávajú využitím funkcií operačných systémov a aplikácií.

|  |  |
| --- | --- |
| **Opatrenie** | **Spôsob využitia** |
| **Ochrana priestorov** | |
| nainštalovaný kamerový systém | obmedzenie a riadenie prístupu osôb |
| nainštalovaný elektronický zabezpečovací systém |
| oddelenie priestorov na spracúvanie osobných údajov - samostatná kancelária |
| písomné dokumenty uložené v uzamykateľných skriniach |
| rozmiestnenie nábytku a počítačov vylučuje odpozeranie osobných údajov z  monitora, prípadne z písomných dokumentov zo stola | ochrana pred náhodným sprístupnením údajov |
| zariadenia na likvidáciu písomných dokumentov | spoľahlivá likvidácia osobných údajov |
| nainštalované hlásiče požiaru a hasiace prístroje | ochrana pred živelnou katastrofou |
| **Automatizované prostriedky spracúvania** | |
| prihlásenie do počítačov vyžaduje meno a heslo používateľa | uplatňovaná povinnosť identifikácie a autentizácie pri prístupe k  informačnému systému, riadenie prístupu k aktívam |
| aplikácie používané na spracúvanie osobných údajov pre spustenie vyžadujú meno a heslo používateľa |
| inštalované opravné programové balíčky pre operačné systémy i aplikácie | zvyšovanie bezpečnosti programového vybavenia |
| ochrana proti škodlivým programom - antivírová ochrana | ochrana proti počítačovým vírusom, pred poškodením údajov, prípadne pred sprístupnením údajov |
| zriadené bezpečné pripojenie na internet – firewall (kontrola, obmedzenie a zamedzenie prepojenia informačných systémov s internetom) | ochrana pred prienikom do počítačovej siete |
| používané záložné napájacie zdroje pre dôležité počítače (sekretariát, recepcia hotelov) | ochrana pre chybami, ktoré môžu nastať pri výpadku el. energie |

**Organizačné opatrenia** zahŕňajú jednoznačné určenie postupov a vzťahov pri ochrane a prevádzke informačného systému.

|  |  |
| --- | --- |
| **Opatrenie** | **Spôsob využitia** |
| **Ochrana priestorov** | |
| vedená evidencia hesiel EZS (u dodávateľa) | obmedzenie a riadenie prístupu osôb |
| **Automatizované prostriedky spracúvania** | |
| pravidelná zmena hesiel | uplatňovaná povinnosť identifikácie a autentizácie, ochrana hesiel |
| odhlasovanie sa z aplikácií i pri dočasnom opustení pracoviska | uplatňovaná povinnosť identifikácie a autentizácie |
| pravidelne vytvorené zálohy | možnosť rýchlej obnovy informačného systému |
| **Interná legislatíva** | |
| vedené evidencie o informačných systémoch | splnenie zákonných požiadaviek |
| spracovaná smernica Ochrana osobných údajov | identifikácia a autentizácia pri prístupe k informačným systémom |
| spracovaný Požiarny štatút | ochrana pred živelnou katastrofou |

**Personálne opatrenia** predstavujú najmä poučenie zamestnancov o jednotlivých interných smerniciach a ich vzdelávanie.

|  |  |
| --- | --- |
| **Opatrenie** | **Spôsob využitia** |
| poučené všetky oprávnené osoby podľa zákona o ochrane osobných údajov | splnenie zákonných požiadaviek, zvyšovanie povedomia o bezpečnosti a potrebe dodržiavať bezpečnostné opatrenia |
| poučení všetci zamestnanci o povinnostiach vyplývajúcich z jednotlivých smerníc |

***Hodnotenie rizík***

STN ISO/IEC TR 13335 definuje tieto možné hrozby: zemetrasenie, povodeň, víchrica, blesk, priemyselná akcia, bombový útok, požiar, úmyselná škoda, prerušenie dodávky el. energie, prerušenie dodávky vody, porucha klimatizácie, porucha hardvéru, kolísanie napájania, extrémna teplota a vlhkosť, prach, elektromagnetická radiácia, elektrostatický náboj, krádež, neoprávnené použitie pamäťového média, poškodenie pamäťového média, chyba zamestnancov – chyba obsluhy, chyba údržby, zlyhanie softvéru, použitie softvéru neautorizovanými užívateľmi, použitie softvéru neautorizovaným spôsobom, predstieranie identity užívateľa, nelegálne používanie softvéru, počítačový vírus – škodlivý softvér, nelegálny import/export softvéru, prístup k sieti neautorizovanými užívateľmi - hackerský útok, použitie sieťového vybavenia neautorizovaným spôsobom, technické zlyhanie sieťových komponentov, chyba prenosu, poškodenie vedenia, preťaženie, odpočúvanie, infiltrácia komunikácií, analýza prevádzky, chybné smerovanie správ, presmerovanie správ, popretie, zlyhanie komunikačných služieb (t.j. sieťových služieb), nedostatok zamestnancov, chyby užívateľov, nesprávne použitie zdrojov.

Na rôzne aktíva (časti) informačných systémov, ktoré sú určené na spracovanie osobných údajov, pôsobia rôzne hrozby. Miera rizika je hodnotená vzhľadom na už realizované bezpečnostné opatrenia. Pre hodnotenie bezpečnosti boli použité nasledujúce kritériá:

Miera rizika:

* nízka – daná hrozba využije zraniteľnosť aktíva len s veľmi malou pravdepodobnosťou, hraničiacou s nulou,
* stredná – pravdepodobnosť uskutočnenia hrozby je významná,
* vysoká – veľmi pravdepodobne sa hrozba uskutoční, s pravdepodobnosťou hraničiacou s jedna, z praktických skúseností vyplýva, že uvedená hrozba často využíva danú zraniteľnosť aktív.

Hodnota dopadu:

* nízka – bez finančných strát, bez porušenia ochrany osobných údajov,
* stredná – dočasné zníženie výkonu APS, finančné straty spôsobené odstraňovaním následkov dopadu do 2 000,- €,
* vysoká – odcudzenie, strata, poškodenie, neoprávnený prístup, zmena alebo šírenie osobných údajov.

Na všetky informačné systémy pôsobia rovnaké možné hrozby. Aktíva jednotlivých informačných systémov sú združené, aby sa popis hrozieb niekoľkonásobne neopakoval.

|  |  |  |  |
| --- | --- | --- | --- |
| **Aktíva informačného systému** | **Hrozby** | **Miera rizika** | **Hodnota dopadu** |
| písomná forma osobných údajov,  písomné dokumenty | požiar | nízka | vysoká |
| úmyselná škoda | nízka | stredná |
| krádež | nízka | vysoká |
| chyba zamestnanca | nízka | stredná |
| dodávka elektrickej energie | požiar | nízka | stredná |
| úmyselná škoda | nízka | stredná |
| chyba údržby | nízka | nízka |
| preťaženie | nízka | nízka |
| počítače určené na spracovanie  osobných údajov | požiar | nízka | vysoká |
| úmyselná škoda | nízka | vysoká |
| porucha hardvéru | nízka | stredná |
| krádež | nízka | vysoká |
| chyba užívateľa | nízka | nízka |
| chyba administrátora | nízka | nízka |
| predstieranie identity užívateľa | nízka | stredná |
| preťaženie | nízka | nízka |
| nainštalované programové vybavenie | úmyselná škoda | nízka | vysoká |
| chyba užívateľa | nízka | nízka |
| chyba administrátora | nízka | stredná |
| použitie softvéru neautorizovanými užívateľmi | nízka | vysoká |
| použitie softvéru neautorizovaným spôsobom | nízka | nízka |
| nelegálne používanie softvéru | nízka | vysoká |
| zlyhanie softvéru | nízka | stredná |
| súbory s osobnými údajmi | úmyselná škoda | nízka | vysoká |
| porucha hardvéru | nízka | stredná |
| krádež | nízka | vysoká |
| neoprávnené použitie pamäťového média | nízka | vysoká |
| chyba užívateľa | nízka | nízka |
| chyba administrátora | nízka | stredná |
| predstieranie identity užívateľa | nízka | vysoká |
| počítačový vírus | nízka | stredná |
| odpočúvanie | nízka | vysoká |
| zariadenie zabezpečujúce pripojenie  na internet | požiar | nízka | nízka |
| úmyselná škoda | nízka | nízka |
| porucha hardvéru | nízka | nízka |
| krádež | nízka | nízka |
| chyba administrátora | nízka | nízka |
| prístup neautorizovaného užívateľa - hackerský útok | nízka | stredná |
| infiltrácia komunikácií | nízka | nízka |

***Vymedzenie okolia informačných systémov***

Organizácia sídli v prenajatých priestoroch, ktoré sú chránené elektronickým zabezpečovacím systémom a monitorované kamerovým systémom. Na spracovanie osobných údajov sa využívajú samostatné kancelárie. Priestory v športovej hale, oddelené od administratívnej časti, využívajú športové kluby.

*Hodnotenia rizika:*

Okolie informačných systémov nemá nepriaznivý vplyv na ich bezpečnosť.

***Vymedzenie zostatkových rizík***

Na základe popisu informačného systému, použitých bezpečnostných opatrení a analýzy rizík bolo posúdené zostatkové riziko.

Voči hrozbe povodne, víchrice, zemetrasenia a terorizmu nie sú priamo vykonané žiadne bezpečnostné opatrenia. Uskutočnenie týchto hrozieb je však veľmi málo pravdepodobné.

Lokalizácia organizácie v záplavovom území môže znamenať v súčasnosti vážne ohrozenie bezpečnosti a významné riziko zničenia informačných systémov a spracúvaných osobných údajov.

Víchrica môže spôsobiť výpadok elektrickej energie a tým dočasnú nedostupnosť osobných údajov, prípadne poškodiť okná a následne technické zariadenia.

Zemetrasenie môže spôsobiť nedostupnosť, prípadne zničenie osobných údajov.

Cieľom terorizmu je násilné poškodenie zariadení, zabitie a zranenie civilných osôb, čo najväčšie narušenie činnosti, vznik neistoty medzi zamestnancami. Môže sa prejaviť uložením výbušniny, vydieraním, braním rukojemníka, výhražnými telefonátmi, poštovými a listovými bombami.

Voči týmto hrozbám sú možné bezpečnostné opatrenia:

* lokalizácia mimo záplavových území,
* regionálne rozloženie organizácie a informačných systémov, rozdelenie do rôznych seizmických pásiem,
* archivácia dokumentov, elektronických dát a záložné APS v inom regióne,
* náhradný zdroj elektrickej energie – generátor.

*Hodnotenia rizika:*

Pravdepodobnosť povodne, ničivej víchrice, zemetrasenia a terorizmu sú veľmi nízke. Organizácia je lokalizovaná mimo záplavových území, informačný systém nie je ohrozený zvýšenou hladinou riek ani prípadnou záplavou. Poškodenie rozvodov elektrickej energie môže dočasne prerušiť prevádzku automatizovaného informačného systému. Miera rizika ohrozenia osobných údajov je však veľmi nízka. Finančné náklady na regionálne rozdelenie archivácie, zálohovania elektronických údajov, prípadne na záložné APS v inom regióne by boli veľmi vysoké a neefektívne. Zostatkové riziko je akceptovateľné.

**Záver**

Slovenský rýchlokorčuliarsky zväz je organizáciou, ktorá má záujem na udržiavaní a rozvoji poskytovaných služieb, na zvyšovaní kvality a na dobrých a korektných vzťahoch so svojimi zamestnancami, obchodnými partnermi a členmi.

Bezpečnostný projekt je zameraný na bezpečnosť spracúvania osobných údajov. Všetky použité bezpečnostné opatrenia však zároveň podporujú i ochranu dobrého mena organizácie a jej rozvoj.

Vývoj informačných systémov a automatizovaného spracúvania informácií je veľmi dynamický a rýchlo meniaci sa proces. Nové programové a technické riešenia prinášajú vyššiu kvalitu, potrebu neustále sa vzdelávať a zároveň pripravovať sa na nové možnosti útokov na ich bezpečnosť.

Kontrola a kontinuálny výkon ochrany zaručia dodržiavanie pravidiel bezpečnosti.